Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method for protecting digital television from unauthorized digital receivers within a population of digital receivers, where each digital receiver in the population has a unique identifier, the method comprising steps of:

at a broadcaster:

receiving provisioning information from a subset of the population of digital receivers indicating that the subset is potentially within range to receive digital television from the broadcaster, the provisioning information including a unique serial number associated with each digital receiver;

distributing first decryption information to the subset of the population of digital receivers, wherein:

the first decryption information allows for potentially decrypting a plurality of programs coextensively in time, and

the unauthorized digital receivers are cryptographically excluded from using the first decryption information;

encrypting first content using a first method using a content encryption key;

distributing the first content;

encrypting the content encryption key using the first decryption information, the first decryption information being generated using the provisioning information; and

distributing the content encryption key to the subset of the population of digital receivers using a second decryption information, wherein the second decryption information is cryptographically secured with the first decryption information.

2. (Previously presented) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further comprising steps of:

encrypting second content using a second method that is cryptographically related to third decryption information, wherein at least one of an algorithm, a key and a key length of the second method is different from that of the first method;

sending the second content; and

distributing third decryption information to the subset of the population of digital receivers, wherein the second decryption information is cryptographically secured with the first decryption information.

3. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further comprising a step of uniquely encrypting the first decryption information for each of the subset, wherein the first-listed distributing step comprises sending first description information uniquely encrypted for each of the subset.

4. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further comprising a step of determining the unauthorized digital receivers to exclude from the subset of the population of digital receivers.

5. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the first decryption information is uniquely encrypted for each of the subset.

6. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the first decryption information comprises a key for decrypting the second decryption information.

7. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the first decryption information expires by changing keys, key lengths and/or algorithms used to encrypt the first content.

8. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each

digital receiver in the population has the unique identifier as recited in claim 1, further comprising a step of forwarding the provisioning information to another broadcaster within range of one of the subset.

9. (Original) The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the unique identifier includes a key.

10. (Cancelled)

11. (Original) A computer system adapted to perform the computer-implementable method for protecting digital television from unauthorized digital receivers within the population of digital receivers of claim 1.

12. (Currently amended) A method for processing digital television within a population of digital receivers, where each digital receiver in the population has a unique identifier, the method comprising steps of:

at a subset of the population of digital receivers:

sending provisioning information from the subset of the population of digital receivers indicating that the subset is within range to receive digital television from a broadcaster, the provisioning information including a unique serial number associated with each digital receiver;

receiving first decryption information by the subset of the population of digital receivers, wherein:

the first decryption information allows for potentially decrypting a plurality of programs coextensively in time, and

the unauthorized digital receivers are cryptographically excluded from using the first decryption information;

receiving first content;

receiving content encryption information from the broadcaster, wherein the content encryption information is encrypted using the first decryption information; and

decrypting the first content using the content encryption information,

wherein the first decryption information is based on the provisioning information,

receiving second decryption information from a place remote to the content receiver, wherein the second decryption information is encrypted using the first decryption information.

13. (Previously Presented) The method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 12, further comprising steps of:

receiving second content;

receiving third decryption information from the broadcaster, wherein the third decryption information is cryptographically secured with the first decryption information; and

decrypting the second content using a second method that is cryptographically related to the third decryption information, wherein at least one of an algorithm, a key and a key length of the second method is different from that of the first method.

14. (Original) The method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 12, wherein the first decryption information is uniquely encrypted for each of the subset.

15. (Original) The method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 12, wherein the unique identifier includes a key.

16. (Canceled)

17. (Original) A computer system adapted to perform the computer-implementable method for processing digital television within the population of digital receivers of claim 12.

Claims 18-31 Canceled.